

FILED

OCT 03 2023

PETER A. MOORE, JR., CLERK
US DISTRICT COURT, EDNC
BY BG DEP CLK

UNITED STATES DISTRICT COURT

for the

Eastern District of North Carolina

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Information from MEGA account JC2828596@gmail.com

Case No. 7:23-mj-1252-RJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

MEGA.nz, Private Bag 92, 533 Victoria Street West, Auckland 1142, New Zealand, as specifically described in Attachment A.

located in the Eastern District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See Attachment B hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

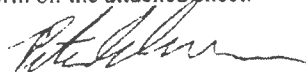
The search is related to a violation of:

| Code Section | Offense Description |
|------------------|---|
| 18 U.S.C. § 2251 | Production Child Pornography |
| 18 U.S.C. § 2252 | Receipt, Distribution and Possession of Child Pornography |

The application is based on these facts:
See attached affidavit which is attached hereto and incorporated herein by reference

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

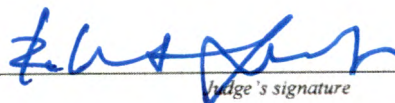
Peter Salomon, Special Agent, NCIS

Printed name and title

On this day, Peter Salomon
appeared before me via reliable electronic means, was
placed under oath, and attested to the contents of this
Application for a Search Warrant.

Date: October 3 2023

City and state: Wilmington, North Carolina



Judge's signature

Robert B. Jones, Jr., United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF
INFORMATION FROM MEGA ACCOUNT
JC2828596@GMAIL.COM TO BE
DOWNLOADED TO COMPUTER MEDIA
IN POSSESSION OF NCIS FROM
SERVERS LOCATED AT PREMISIES
CONTROLLED BY MEGA.NZ

Case No. 7:23-mj-1252-RJ

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Peter Salomon being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. **Affiant:** I am a Special Agent with the Naval Criminal Investigative Service (NCIS) and have been since January 2019 and am currently assigned to Resident Agency Cherry Point, North Carolina. I was previously retained as a contractor by the United States Office of Personnel Management from 2016-2018 as an Investigator. I graduated from Mount St. Mary's University with a Bachelor's of Science in Business. I am a graduate of the Criminal Investigator Training Program (CITP) and the NCIS Special Agent Basic Training Program located at the Federal Law Enforcement Training Center in Glynco, Georgia. Since graduation from CITP, I worked a variety of criminal investigations. Through training and experience, I have become familiar with methods and schemes utilized to possess, produce and distribute child pornography. I have received organized and on-the-job training in multiple disciplines and investigative techniques utilized during criminal investigations. As part of my daily duties as a NCIS Special Agent, I investigate violations of the Uniform Code of Military Justice and Federal Crimes. I am authorized to execute warrants issued under the authority of the United States.

2. **Information provided:** The statements in this affidavit are based on my personal observations, my training and experience, my investigation of this matter, and information obtained from other Agents, law enforcement officers, and witnesses. Because this affidavit is being submitted for the limited purpose of securing search and seizure warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that fruits, evidence, and instrumentalities of the unlawful receipt, distribution, and possession of child pornography also known as Child Sexual Abuse Material (CSAM) are located in the following places or devices:

- a. MEGA account(s) associated with username/email(s): jc2828596@gmail.com.

3. **Requested action:** I make this affidavit in support of an application for a search warrant for the user account(s), listed above, which are more particularly described in **Attachment A** and the seizure and search of the items described in **Attachment B**. Specifically, this Affiant is seeking judicial permission to attempt to login to the MEGA account(s) associated with username/email(s): jc2828596@gmail.com with the password [carter8030] and to search and seize all data contained in this account. The Affiant is also seeking an order to MEGA to provide certain information and take specific actions listed in **Attachment B**.

4. **Jurisdiction:** This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

5. **Sexual Exploitation / Attempt Sexual Exploitation of a Child, 18 U.S.C. § 2251(a) and (e):** Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who

transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed. It is also a crime to attempt to commit this crime.

6. **Receipt and Distribution of Child Pornography: 18 U.S.C. § 2252(a)(2):** This investigation concerns alleged violations of 18 U.S.C. § 2252(a)(2), which prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

7. **Possession of Child Pornography: 18 U.S.C. § 2252(a)(4):** This investigation concerns alleged violations of 18 U.S.C. § 2252(a)(4), which prohibits a person from knowingly possessing, or knowingly accessing with intent to view, any visual depiction of minors engaging in sexually explicit conduct when such visual depiction while in the special maritime and

territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the Government of the United States. 18 U.S.C. § 2252(a)(4), also prohibits knowingly possessing, or knowingly accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

8. **Definitions:** The following definitions apply to this Affidavit and its

Attachments:

- a. The term “minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
- b. The term “sexually explicit conduct,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.
- c. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

9. **MEGA:** MEGA is a cloud storage and file hosting service offered by MEGA Limited, a company in New Zealand. MEGA provides user-controlled encrypted cloud storage

through a web browsers and applications. MEGA is known for its security feature where all files are end-to-end encrypted locally before they are uploaded.

BACKGROUND OF THE INVESTIGATION

10. **Investigation of PAUL (REYES):** On 28May23, The North Carolina State Bureau of Investigation (NCSBI) received information through the National Center for Missing and Exploited Children (NCMEC) that had been reported by Instagram, LLC regarding “Apparent Child Pornography” being uploaded to the platform, which was documented in NCMEC CyberTip report 162882393.

11. The CyberTip was generated and submitted to NCMEC by Instagram on the belief that the reported files depicted Child Sexual Exploitation (CSE) through some type of review, matching algorithm, file names, or other indicators.

12. NCMEC was established in 1984 as a private, nonprofit 501(c)(3) organization. NCMEC provides services nationwide to families and professionals relating to preventing the abduction and sexual exploitation of children. Pursuant to its mission and congressional authorization (see 42 U.S.C. § 5773), NCMEC operates the CyberTip line and the Child Victim Identification Program to provide assistance to law enforcement in its efforts to identify victims of child pornography and child sexual exploitation.

13. NCMEC also works with law enforcement officers, Electronic Service Providers, electronic payment service providers and others in their efforts to reduce the distribution of child sexual exploitation images and videos on the Internet. NCMEC does not investigate and cannot verify the accuracy of information it receives. NCMEC forwards reports of possible child sexual exploitation to law enforcement for its independent review and analysis. This Affiant has previously participated in investigations involving CyberTips from the NCMEC.

14. On 20Jun23, NCIS received a PDF file of CyberTip report number 162882393. The report indicated Electronic Service Provider (ESP) Instagram, Inc (Instagram) was the reporting party. The report was initially received by the NCSBI who forwarded it to NCIS. Instagram reported suspected child pornography files were uploaded by ESP User ID: 52590553515 on 05-25-2023 03:25:08 UTC. The suspect was identified in the NCMEC report as "oren.tanium" and showed an Instagram verified email address of orentanium642@gmail.com. On 15Jun23, NCSBI had obtained a subpoena for the IP address: 2603:6081:3:7b7a:6d47:1816:44:6193 listed in the CyberTip report, which revealed the subscriber was "Paul Reyes", with a service and billing address of 4868 Barracks, Apt 118B, Cherry Point, NC 28533. MCAS Cherry Point, NC is located in the Eastern District of North Carolina.

15. Your Affiant researched and identified LCpl Paul REYES (REYES), USMC, Marine Corps Air Station (MCAS) Cherry Point, NC. The CyberTip indicated five files were uploaded by REYES to Instagram. One file was flagged as a prepubescent minor engaged in a sex act and four files were flagged as a pubescent minor engaged in a sex act. NCEMC indicated in the report they did not review the files, but had flagged the content as child pornography based on a "Hash Match". Instagram provided NCMEC with an MD5 has value (a digital fingerprint) for each of the five files uploaded, to their platform as well as a copy of the files themselves.

16. On 27Jun23, your Affiant obtained Command Authorization for Search and Seizure (CASS), the military equivalent to a search warrant, to review the files accompanying the CyberTip as they were stored with NCIS aboard MCAS Cherry Point, NC, but had not yet been reviewed. After obtaining the signed CASS, review of the files revealed there were five videos containing apparent child pornography uploaded to

Instagram by user "oren.tanium". Your Affiant detailed review of three of the videos revealing the following information:

a. **Video file**

"UMtVeXE0s55EAD32349153009_6083185321766515_8637741154213800917_n" depicted a one minute and sixteen second video depicting an apparent minor bent over on a bed with her pants and underwear pulled down, while wearing a white and blue shirt. The viewer can see her exposed vagina and anus. An adult male wearing pinkish underwear presses his penis against her backside through his underwear. The male pulls down his underwear and penetrates the minor female's anus with his penis. During the video a child can be heard crying in the background.

b. **Video file**

"w7tPBh6M0EE35N0m348478374_4961645390626739_2560914881312273547_n" depicted a one minute and eighteen second video depicting an apparent minor male and apparent minor female kissing. The video switches and one minor female is kissing a minor male, while another minor female has the erect penis of the minor male in her mouth. A possible adult female is stroking the scrotum of the minor male.

c. **Video file**

"b5wbmb6bFEHBWzDs348781830_6475166602562900_8588190100329159293_n" depicted a thirty-four second video depicting an apparent minor female sitting on the floor in front of a couch. The girl's vagina is exposed. An adult male forces his penis into her mouth and shoves it in and out of her mouth.

17. On 07Aug23, your Affiant interrogated REYES pertaining to his alleged involvement in receipt, possession, and distribution of child pornography. Prior to the interrogation, REYES was advised of his Military Suspect's Acknowledgement Waiver Rights (Article 31B). REYES stated he understood, waived his rights, and signed the rights waiver form. REYES provided he started "experimenting" with child pornography for a few months to see what would sexually arouse him. REYES provided he tried to masturbate to the child pornography videos but told your affiant it was not really working for him. REYES received the child pornography videos from unknown persons online and knew the videos contained child pornography because the link to click would contain information on what the videos were of. REYES provided he distributed CSAM by sending free links and stated he sent videos more than one time to unknown people online. REYES provided he previously had a MEGA account but provided it was deleted a few months prior by MEGA. REYES did not provide specifics about what was in his MEGA account or any of the account information. REYES admitted to using the previously mentioned Instagram account to send and receive CSAM. REYES voluntarily provided his phone passcode and admitted there was CSAM on his phone.

18. On 07Aug23, your Affiant obtained a CASS for REYES' cell phone, barracks room and all electronic devices contained within to search and seize evidence pertaining to REYES's alleged involvement in possession, receipt, and distribution of child pornography.

19. On 07Aug23, multiple electronic devices were seized from REYES' barracks room to include two iPhones. Your Affiant extracted one cell phone and placed a copy of the extraction in evidence. NCIS Digital Forensic Examiner (DFE) Richard Novelli extracted the other phone and completed an examination of contents from both phones for CSAM and located over 300 CSAM videos and over 1000 CSAM images of minor girls, the majority of whom

appeared to be younger than 12 years of age. The observed CSAM included images and videos of infants and toddlers being sexually abused.

20. Your Affiant reviewed some of the images from REYES' cell phone and located two thumbnail images dated 21May23. The thumbnail images matched parts of the content previously observed from Video file "w7tPBh6M0EE35N0m348478374_4961645390626739_2560914881312273547_n" and from Video file "b5wbmb6bFEHBWzDs348781830_6475166602562900_8588190100329159293_n", which were previously identified as having been sent by REYES via Instagram in the NCMEC CyberTip report.

21. On 15Sep23, DFE Novelli reviewed images from REYES cell phone and located a photograph of the MEGA.nz login page. The image was in the "Notes" section of the phone and depicted the account email jc2828596@gmail.com. DFE Novelli located in REYES phone a safari internet browser Google "cookie" showing jc2828596@gmail.com was an account used on the phone browser. DFE Novelli located another screenshot on REYES device showing a login to a Google account in the name "John Carter" who utilized email address jc2828596@gmail.com.

22. Your Affiant requested and received documentation for user account information from MEGA for account(s) associated with email address jc2828596@gmail.com. MEGA provided subscriber information which revealed jc2828596@gmail.com was tied to the name "John Carter" with email address jc2828596@gmail.com. The MEGA account was created on February 21, 2023. The account had 61 active public links. Your Affiant believed these MEGA links could be sent or posted making the linked content accessible for anyone with a copy of the

link. The account was last accessed on June 25, 2023. The account contained over 11 GB of data to include "1239" files in "3" folders. The account had 9 deleted files and 0 deleted folders. MEGA purge protected the account from possible deletion at your Affiant's request.

23. I reviewed the IP address logs received from MEGA for the MEGA account jc2828596@gmail.com and observed that on or about 24May23, the account was logged into through IP address: 2603:6081:3:7b7a:6d47:1816:44:6193, which fell within IP address lease dates on the subpoena received from NCSBI, which revealed the subscriber for the IP address at the time was REYES.

24. **Evidence from the Accounts in Question:** In my training and experience, evidence of who was using applications (such as a Google and MEGA accounts) and from where the applications were being used, as well as evidence related to criminal activity of the kind described above, are likely to be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

- a. **Direct Evidence of Criminal Activity:** For example, the stored communications and files connected to the online and application accounts may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.
- b. **Attribution Evidence:** In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google, Inc. and MEGA

can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

- c. **State of Mind / Intent:** Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).
- d. **Discovery of Additional Evidence and Criminal Activity:** Other information connected to the accounts requested may lead to the discovery of additional evidence. For example, the accounts may reveal other minor victims used in furtherance of the crimes under investigation or other on-line applications used to communicate with co-conspirators. In addition, instant messages, Internet

activity, documents, and contact information can lead to the identification of unidentified minor victims and co-conspirators and instrumentalities of the crimes under investigation.

25. Based on my own training and experience in investigating computer-facilitated child sexual exploitation crimes, and the experiences of other law enforcement agents with whom I have consulted; I believe the majority of individuals who sexually exploit children or collect child pornography via the Internet maintain their collections, increasingly in both online and offline storage media, even as they relocate from one residential or work address to another. Sexually explicit images and videos of minor children engaged in sexually explicit conduct and/or with their genitals exposed were recovered from two different cell phones belonging to REYES. Screenshots and images in REYES phone show he used a MEGA account and MEGA records show REYES had 61 active public links. Furthermore, DFE Novelli located an image in REYES phone of what appeared to be MEGA subfolders under the main folder "2023 NEW COLLECTION". Some of the subfolders were entitled: Child rape, FULL LENGTH CP, INDIAN CP, KIDS TOGETHER, Mix Cp, PURE CP, and sexy cp.

26. Based on evidence REYES was using application Instagram to communicate with others to distribute and receive sexually explicit visual depictions of minors, it is also believed that he may have shared or received files through other means. In this Affiant's experience, persons who engage in trading this type of material will also use other avenues to obtain sexually explicit files. This Affiant has probable cause to believe that information regarding these accounts and information requested in **Attachment B** will be necessary to identify the individuals involved.

27. **MEGA:** MEGA, Limited is New Zealand based user encrypted cloud service

provider. Specifically, MEGA provides secure cloud storage and communication platform with user-controlled end-to-end encryption. End-to-end encryption means that no intermediary- not even MEGA - has access to the user's encryption keys and therefore the stored data. However, users have the option to share data (individual files or entire folders), plus the associated encryption keys, with others. Access to MEGA is primarily through web-based apps. MEGA mobile apps are also available for Windows Phone, Android and iOS.

- a. MEGA provides new (basic) users with a complimentary 50 gigabytes of free cloud storage for the first month. After which time, the storage capacity shrinks to 15 gigabytes. A basic user can activate additional storage allowances through various "achievements", but these earned storage allowances also expire. The completion of achievements include: installing the desktop client and the mobile app – allowing extra storage for 180 days; inviting friends to create a MEGA account – provides user with additional storage for a year. The maximum permanent storage for a basic user is 50 gigabytes. MEGA's free service provides 10 gigabyte band-width, which refills every thirty (30) minutes. This bandwidth restriction means a user can upload/download to/from the user's account to an extent which is not more than 10 gigabytes. MEGA offers four (4) premium plans to paid users. MEGA offers instant downloads at the same speeds to all users, whether they are a premium user or not. MEGA only restricts downloads when the user has reached a certain bandwidth limit each month.
- b. **Sharing files on MEGA:** MEGA users can share a folder or individual files from their MEGA account by generating a Public URL. This Public URL (or MEGA link) is a direct link to a MEGA user's file(s) or folder(s). The MEGA user can

then share this MEGA link via email or SMS. Anyone with the MEGA link, including a person who does not have a MEGA account, has the ability to download the shared content without the need for the MEGA user's username and password.

- i. There are pros and cons to generating and sharing MEGA links.
 - ii. The pros being it is very flexible sharing, easy to use, and anyone can access the content of the shared link.
 - iii. The cons being once the MEGA link has been shared, anyone who has the link can download the user's file(s) and/or folder(s).
- c. MEGA also offers a user the ability to communicate with other MEGA users via chat, voice, and video – called MEGAchats. This communication is encrypted and cannot be intercepted by MEGA. MEGA users can also create and manage a list of contacts within the application.
- d. MEGA Limited is a New Zealand company which maintains a cooperative relationship with international enforcement authorities. They have zero-tolerance for Child Sexual Abuse Material and voluntarily disclose all available information to authorities. All files stored in MEGA are fully encrypted at the user's device so the files are unable to read unless law enforcement logs into the account with the user's password or if law enforcement has been given a file/folder link with the encryption key included.

28. **Collection behavior:** This Affiant also has probable cause to believe that the account listed in **Attachment A** may contain contraband, specifically images of minors engaged in sexually explicit conduct, based on collection behavior of individuals who are sexually

attracted to children.

- a. I have been informed of the studies of child sex offenders in general, and child pornography offenders in particular. I have learned about the activities and characteristics of child pornography offenders from other law enforcement agents who focus on online child sexual exploitation, including those who investigate the offenses and those who analyze the computer equipment of the offenders.
- b. Based on my own experience and what I have learned from other individuals who specialize in the investigation and study of child pornography offenders, I know that the following traits and characteristics are generally found to exist and be true in cases involving individuals who sexually exploit children or collect child pornography:
 - i. The majority of individuals who sexually exploit children or collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.
 - ii. The majority of individuals who sexually exploit children or collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

- iii. The majority of individuals who sexually exploit children or collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.
- iv. The majority of individuals who sexually exploit children or collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials.
- v. Based on my own experience in investigating computer-facilitated child sexual exploitation crimes, and the experiences of other law enforcement agents with who I have consulted, I believe that the majority of individuals who sexually exploit children or collect child pornography via the Internet maintain their collections, increasingly in both online and offline storage media, even as they relocate from one residential or work address to another.

CONDITION REQUIRED PRIOR TO EXECUTION

29. NCIS Special Agents, other Special Agents, law enforcement officers and Representatives thereof deemed necessary for execution of this warrant; plan on accessing the MEGA account using REYES login credentials and historic passwords if necessary. The account password and possibly email address will be changed by law enforcement prior to

extraction/download of the account contents to avoid possible tampering or evidence destruction by REYES. If access is successfully obtained, either MEGA's data transfer tool or other cyber tools will be utilized to extract/download the account's information onto computer media in possession of NCIS or law enforcement representatives located in the Eastern District of North Carolina. The downloaded information may include, but is not limited to, files, communications, deleted folders, and contact lists associated with the Target Account.

30. Your Affiant is seeking permission to search the Target Account following the triggering event of the download of said information by NCIS as described in **Attachment A**, and to seize the items and information described in **Attachment B**.

31. **Manner of execution:** Because this warrant seeks permission only to examine information on computer media in law enforcement's possession, the execution for this warrant does not involve physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

32. **Nature of examination:** Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Data consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Data to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

33. Based upon the contents of this Affidavit, your Affiant respectfully submits there is probable cause to believe that contraband, evidence, fruits, and/or instrumentalities of the violations of the subject offenses, specifically those items more fully set forth in **Attachment B**, are currently located in the Target Account described in **Attachment A**, and will be located in

the Target Account as a result of this warrant. Therefore, I respectfully request that the Court issue a search warrant for the Target Account.

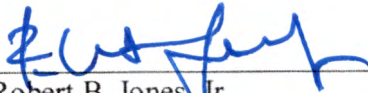
Respectfully submitted,



Peter Salomon
Special Agent
Naval Criminal Investigative Service

On this day, Peter Salomon appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this Affidavit.

This 3 day of October, 2023.



Robert B. Jones, Jr.
United States Magistrate Judge
Eastern District of North Carolina.

ATTACHMENT A

DESCRIPTION OF ITEMS TO BE SEARCHED

This warrant applies to information associated with the following MEGA.NZ account:

Account(s) associated with username/email: jc2828596@gmail.com. The contents of this account are stored at premises owned, maintained, controlled, or operated by MEGA.nz, a company headquarters at Private Bag 92, 533 Victoria Street West, Auckland 1142, New Zealand. This warrant applies to the data to be downloaded as a result of this warrant to computer media in possession of the Naval Criminal Investigative Service located in the Eastern District of North Carolina from MEGA.nz servers in New Zealand.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED AND SEARCHED

All account data including but not limited to: messages, contacts, metadata, links, and files, to include recoverable deleted files associated with MEGA account tied to jc2828596@gmail.com with the password [carter8030].

Evidence and instrumentalities concerning violation(s) of Title 18, United States Code, Sections pertaining to possession, distribution, production, or transportation of visual depictions of minors engaged in sexually explicit conduct.

Information relating to the identities and locations of any persona who created or used the account; or who communicated with the account, if the communications pertained to the possession, receipt, transportation, production, or distribution of minors engaged in sexually explicit conduct, as defined in 18 USC § 2256(2)(A).